

AMETAS

Good Migrations.

AMETAS White Paper Series

by Klaus Herrmann
and Michael Zapf

On Interfaces

July 2000

Johann Wolfgang Goethe-Universität Frankfurt/Main, Germany
Department of Computer Science

www.ametas.de

Getting In Contact With Your Place

This paper describes how users can get in contact with an agent place in the agent system AMETAS.

I Started a Place — and Now?

So you've actually managed to configure a place so that it seems running. Congratulations! Now you would like to start some agents that you have already prepared. The manual states that Place Users are normally activated by a special driver method call of another Place User. But somewhere there must be a beginning, a *first* Place User you communicate with.

The AMETAS Attachable Interface (AMAI)

In order to get in first contact with a place, you normally use AMAI. Every place accepts multiple connections by these interfaces that may be attached and detached during run-time of the place. AMAI may establish a connection to a place from any host; it need not be collocated with the place.

Using AMAI, a human user is actually *not* integrated in the agent system. That means it is impossible for him to receive messages from other Place Users, including his own agents. Therefore, AMAI should only be used to start up a user adapter which then integrates the user correctly. Figure 1 shows the typical AMAI main window.

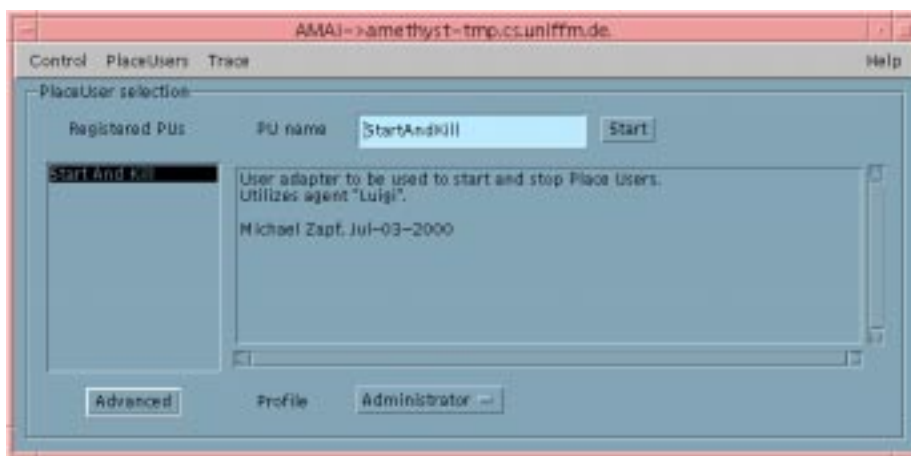


Figure 1: AMAI main window

User Tasks

AMAI is mainly used to start user adapters. Of course, agents and even services may be started by AMAI, but the user cannot provide any messages or other parameters for their initialization. Therefore, if agents or services are to be started by AMAI, they must not expect an initialization message.

The normal procedure is to connect to a place which requires to user to provide three entries:

- the place name to connect to;
- a user identity file name;
- a passphrase to unlock the private key inside the identity file.

The user identity file must have been created before, using a security tool like *SecAdmin*. When the secret key is correct, the connection is established. The user may now start Place Users that need to be locally installed at that place, i.e. they must be available in special container files in the corresponding directory of the file system of the host where the place is running.

When the Place User is started, the private key is used to create a signature that accompanies the Place User when it migrates (in case of an agent). When the user adapter starts an agent, this agent is also signed using the private key.

AMAI allows the user to take a look at the log file of the place, but only at log entries coming from the agent or the place. Debug messages cannot be inspected by a normal user. This task requires administrative privileges.

When the user connects to a place for the first time, he needs to enter the file name of his identity file and the corresponding passphrase. These data are saved in a file that is stored on the local file system of the host where AMAI is running. To prevent security breaches, the whole file is encrypted before it is stored. The user must provide a second passphrase to allow the decryption of the file at the next start of AMAI. When the user connects to the same place at a later time, the entries are retrieved and automatically used for logging in.

Administrative Tasks

AMAI is also designed for administrators who want to check what is happening inside a place. In some cases this might be the only chance to find out what is going wrong. Unlike normal users, the administrator may look at debug data that is much more detailed than the publicly available data. Tasks that are reserved to be used by administrators are

- starting Place Users with administrative privileges;
- looking at debug data from the place log file;
- inspecting maintenance data like message queue sizes, available Place Users, or registered event listeners;
- viewing configuration data of the place and reconfiguring it;
- registering and deregistering Place Users at the place;
- stopping the place.

Stopping the place seems to be a convenient way of getting your malfunctioning agent application under control, but it cannot be recommended as an everyday strategy. This severe intervention not only entails the termination of any running Place User on this place but also the unavailability of this place as a migration target. However, this is the normal case with temporary places; the owner of a temporary place should therefore have administrative privileges.

Place Users may depend on the set of privileges that their user will be granted at the current place. When logged in as an administrator, a user can launch an agent that can kill any other Place User; but with normal user privileges it may only kill his own agents.

Security

Security in AMETAS is a special issue that is treated in a separate paper in the *AMETAS White Paper Series*. AMAI needs to provide as good security precautions as the rest of AMETAS so that it does not become a *weakest link* to be broken by attackers.

When AMAI connects to a place, both communication ends create an encrypted channel that is used throughout the time of connection with this place. This is achieved by the place sending a session key encrypted with the user's public key. Only in case the user knows the passphrase belonging to the identity that contains this key, the symmetrically encrypted connection is established successfully. From now on, all communication will use this encrypted channel.

The user can choose to have his identities and passphrases stored in a file on the local file system. For the purpose of encryption, the user must provide another passphrase that must be used again once at every restart of AMAI. In that file, a mapping is defined between the place name and the pair of identity file name and corresponding passphrase so that whenever you connect to a certain place, AMAI looks up these data in relation to the place name, and when it finds the entries, it uses them for connecting the user to the place without requiring the user to retype his identity and passphrase.

When the user connects to a place, this place determines the maximum set of privileges that Place Users started by this user will be granted. That means that in order to gain special privileges, it is required to define a special identity that is granted these privileges at the place and to use it in subsequent connection attempts with AMAI. Having administrative privileges at one place does not imply having those privileges elsewhere. You may read more about privileges in the corresponding paper of the *AMETAS White Paper Series*.

Profile Management

A profile in AMAI is a mapping of place name to the pair of identity file and corresponding passphrase. As long as one profile is used, the same identity is used when trying to connect to a place. However, the user could desire to log in the place as an administrator. In this case it is possible to define another profile that uses another mapping. AMAI allows you to define numerous profiles which can be identified by a name. Figure 2 demonstrates the mapping of place names to authentication data for the respective profile.

Places	MyPlace1	shopping	office	meeting
Standard	(Idy1; bgu7z)	(Idy1; bgu7z)	(Idy2; dfjdk)	(Idy1; bgu7z)
Administrator	(AdmIdy; udh887)	-	-	-

Figure 2: Profiles

The profile named *Standard* is always available but is empty at the first start. The mapping is automatically updated whenever a new connection to a place is created successfully. In order to allow connections as an administrator, it is just necessary to

create a profile named e.g. *Administrator* and give the correct entries at each connection attempt. Profile names are only meaningful for AMAI; you will only get administrative privileges if the *domain access policy* of the place you connect to is adequately defined.

Begone, Ye Wicked Graphical Stuff!

You need not hate graphics when you decide not to use AMAI. For example, you could have an X server redirection that is slow or you just want to start a user adapter quickly. This is where AMSI comes into the spotlight.

AMSI is short for AMETAS Simple Interface which is purely text-based and therefore also available for use on text terminals. AMSI has the following restrictions:

- It does not use graphical display;
- it does not offer log inspection;
- it does not offer place configuration inspection and modification;
- it does not provide Place User registration or deregistration;
- it does not use profiles.

But it has quite some advantages over AMAI:

- It can be easily used to launch Place Users;
- it can be used inside scripts.

All actions are triggered by textual commands. These commands can also be used as command line parameters at the start of AMSI. You can create a shell script (or batch file in Windows) and start AMSI together with commands and parameters in one line. When all necessary parameters were provided, AMSI performs the requested action and directly returns. This way you can create an easy-to-remember command file to start-up your agent application! Figure 3 shows a possible output of a session with AMSI.

```
AMSI> connect myplace.dom.de.  
Passphrase: .....  
myplace.dom.de.> inspect eventlisteners  
  ID: MESSAGE_RECEIVED_EVENT: none  
  ID: MESSAGE_REMOVED_EVENT: none  
  ID: PU_EVENTS: none  
  ID: PLACE_EVENTS: none  
myplace.dom.de.> start StartAndKill  
myplace.dom.de.> inspect placeusers  
  Running: StartAndKill|MZUA|940301a1000000e0b...  
myplace.dom.de.> quit
```

Figure 3: AMSI session

In order to build up the connection, AMSI uses the identity file name and corresponding passphrase for authentication at the place. These data can again be stored in AMSI's configuration file. You can also write the passphrase in the file but this is not recommended because the file will not be encrypted. On your home PC, you could

consider to tolerate this security risk. Although AMSI does not support profiles, you can log-in using different identities by replacing the configuration file of AMSI before starting it. Like AMAI, AMSI utilizes an encrypted connection to a place so that your passphrase will not be compromised.